UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,518	12/03/2003	Isao Watanabe	04329.3188	5006

22852 7590 01/10/2007

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
FEARER, MARK D	
ART UNIT	**PAPER NUMBER**
2112	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/725,518	WATANABE, ISAO	
	Examiner	Art Unit	
	Mark D. Fearer	2112	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *December 3, 2003, May 23, 2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

The information disclosure statements submitted on 03December2003 and 23May2005 have been considered by the Examiner and made of record in the application file.

Specification

Claim 1 objected to because of the following informalities: in the Detailed Description of the Invention, page 9, line 10, network segment 21 is referred to, which does not exist. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

a. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1 – 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamill-Keays et al. (US patent 6223046) in view of Johnson et al. ('Mobility Support in Ipv6').

Consider claim 1, Hamill-Keays et al. clearly shows and discloses a service control point for forwarding a communication request, which is directed to a node and is transmitted from another node, to a network segment to which the node is currently connected. This reads on the claimed "An apparatus for forwarding a communication request, which is directed to a home address of a mobile node and is transmitted from another node via a network, to a network segment to which the mobile node is currently connected..." ("When attempts to contact a mobile terminal directly by different applications are unsuccessful, a control node, such as a Home Location Register (HLR) or a Service Control Point (SCP) within an Intelligent Network (IN), can receive notification requests from these nodes or applications and prioritize them according to

the time received and/or the priority of each requesting application." abstract). This request is normally made to a control point in the network which stores data indicating the address of the party or application who requires notification. This reads on the claimed "... informing unit configured to executes, based on the stored event information, a process for informing said another node via the network that the mobile node has become communicable, ... which is transmitted via the network from the mobile node connected to the network segment" ("An alternative to this is for the party or application to request the network 10 to notify it of when the MS 20 is known to be available, for example, at power on, location registration, or contact by another party." column 2, lines 10 – 13). However, Hamill-Keays et al. fails to limit the specifics of IP networks. Johnson et al. discloses a system for forwarding a communication request in which each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. This reads on the claimed "An apparatus for forwarding a communication request, ...based on a relationship between the home address and a care-of-address used in the network segment" ("IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of address. The protocol enables IPv6 nodes to cache the binding of a mobile node's home address with its care-of address, and to then send packets destined for the mobile node directly to it at this care-of address." abstract). Further, an informing unit configured to execute, based on the stored event information, a process for informing said another node via the network

that the mobile node has become communicable, in response to a registration request for registration of the care-of-address, which is transmitted via the network from the mobile node connected to the network segment. This reads on the claimed "... a process for informing said another node via the network that the mobile node has become communicable, in response to a registration request for registration of the care-of-address, which is transmitted via the network from the mobile node connected to the network segment" ("After detecting that its link-layer point of attachment has moved from one IPv6 subnet to another (i.e., its current default router has become unreachable and it has discovered a new default router), a mobile node SHOULD form a new primary care-of address using one of the on-link network prefixes advertised by the new router." (see 8.3. Forming New Care-of Addresses)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate IPv6 packets addressed to a mobile node's home address being transparently routed to its care-of address and the protocol enabling IPv6 nodes to cache the binding of a mobile node's home address with its care-of address, and then sending packets destined for the mobile node directly to it at this care-of address as taught by Johnson et al with service control point as shown by Hamill-Keays et al. for the purpose of an apparatus that forwards communication requests directed to a home address of a mobile node and transmitted from another node via a network, to a network segment to which the mobile node is currently connected, based on a relationship between the home address and a care-of-address used in the network segment.

Consider claim 2, Hamill-Keays et al. clearly shows and discloses an apparatus according to claim 1, further comprising a unit that stores the address of the party or application who requires notification. This reads on the claimed "... apparatus according to claim 1, further comprising a unit that stores the ...address of the mobile node ..." ("This request is normally made to a control point (not shown) in the network 10 which stores data indicating the address of the party or application who requires notification." column 2, lines 13 - 16). However, Hamill-Keays et al. fails to teach registered care-of addresses. Johnson et al. discloses a system in which each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. This reads on the claimed "... care-of-address of the mobile node on the basis of the registration request for the care-of-address." ("Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location." abstract).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a control point in a system in which each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet, or while situated away from its home, a mobile node is also

associated with a care-of address, which provides information about the mobile node's current location as taught by Johnson et al. as the control point which stores data indicating the address of the party or application who requires notification as shown by Hamill-Keays et al. for the purpose of a unit that stores the care-of-address of the mobile node on the basis of the registration request for the care-of-address.

Consider claim 3, Hamill-Keays et al., as modified by Johnson et al., clearly shows and discloses an apparatus according to claim 1 wherein the event information includes an address of said another node that has transmitted the communication request ("When the MS 440 powers on (step 520) and the HLR 430 detects activity, the HLR 430 scans the list of notification requests 435 for the subscriber trying to detect a priority one notification (step 525)." column 4 line 63 and column 5 line 10).

Consider claim 4, Hamill-Keays et al. clearly shows and discloses a system in which priorities between different applications can be set and intervals between notifications can be controlled to values appropriate for the requesting applications in order to provide an efficient and effective system and method for coordinating notification requests. This reads on the claimed "means for executing a ... process ..., wherein the informing unit includes a unit that executes said process ..., after the validity check process ..." ("Thus, priorities between different applications can be set and intervals between notifications can be controlled to values appropriate for the requesting applications in order to provide an efficient and effective system and method

for coordinating notification requests." abstract). However, Hamill-Keays et al. fails to teach validity checks for determining whether the registration request is valid, in response to the registration request for the care-of-address. Johnson et al. discloses a system for validating registration requests if the packet contains an IP authentication header and the authentication is valid. The authentication header MUST provide sender authentication, integrity protection, and replay protection. The option length field in the binding update option is greater than or equal to the specified length. The sequence number field in the binding update option is greater than the sequence number received in the previous binding update for this home address, if any. The sequence number comparison is performed modulo 2**16. The packet MUST contain a valid home address option. The home address for the binding is specified by the home address field of the home address option. This reads on the claimed "...means for executing a validity check process for determining whether the registration request is valid, in response to the registration request for the care-of-address, ... ("Upon receiving a Binding Update option in some packet, the receiving node MUST validate the Binding Update according to the following tests: The packet contains an IP Authentication header and the authentication is valid [1]. The Authentication header MUST provide sender authentication, integrity protection, and replay protection. The Option Length field in the Binding Update option is greater than or equal to the length specified in Section 4.1. The Sequence Number field in the Binding Update option is greater than the Sequence Number received in the previous Binding Update for this home address, if any. The Sequence Number comparison is performed modulo 2**16. The packet MUST

contain a valid Home Address option. The home address for the binding is specified by the Home Address field of the Home Address option." (see 'Mobility Support in Ipv6', 6.2. Receiving Binding Updates)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a system for validating registration requests if the packet contains an IP authentication header and the authentication is valid as taught by Johnson et al. with priorities between different applications being set and intervals between notifications being controlled by values appropriate for the requesting applications in order to provide an efficient and effective system and method for coordinating notification requests as shown by Hamill-Keays et al. for the purpose of executing a validity check process for determining whether the registration request is valid, in response to the registration request for the care-of-address, wherein the informing unit includes a unit that executes said process for informing, after the validity check process determines that the registration request is valid.

Consider claim 5, Hamill-Keays et al. clearly shows and discloses a system in which priorities between different applications can be set and intervals between notifications can be controlled to values appropriate for the requesting applications in order to provide an efficient and effective system and method for coordinating notification requests. This reads on the claimed "means for executing a ... process ..., wherein the informing unit includes a unit that executes said process ..., before the validity check process is executed ..." ("Thus, priorities between different applications

can be set and intervals between notifications can be controlled to values appropriate for the requesting applications in order to provide an efficient and effective system and method for coordinating notification requests." abstract). However, Hamill-Keays et al. fails to teach validity checks for determining whether the registration request is valid, in response to the registration request for the care-of-address. Johnson et al. discloses a system for validating registration requests if the packet contains an IP authentication header and the authentication is valid. The authentication header MUST provide sender authentication, integrity protection, and replay protection. The option length field in the binding update option is greater than or equal to the specified length. The sequence number field in the binding update option is greater than the sequence number received in the previous binding update for this home address, if any. The sequence number comparison is performed modulo 2**16. The packet MUST contain a valid home address option. The home address for the binding is specified by the home address field of the home address option. This reads on the claimed "...means for executing a validity check process for determining whether the registration request is valid, in response to the registration request for the care-of-address, ... ("Upon receiving a Binding Update option in some packet, the receiving node MUST validate the Binding Update according to the following tests: The packet contains an IP Authentication header and the authentication is valid [1]. The Authentication header MUST provide sender authentication, integrity protection, and replay protection. The Option Length field in the Binding Update option is greater than or equal to the length specified in Section 4.1. The Sequence Number field in the Binding Update option is greater than

the Sequence Number received in the previous Binding Update for this home address, if any. The Sequence Number comparison is performed modulo 2**16. The packet MUST contain a valid Home Address option. The home address for the binding is specified by the Home Address field of the Home Address option." (see 'Mobility Support in Ipv6', 6.2. Receiving Binding Updates)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a system for validating registration requests if the packet contains an IP authentication header and the authentication is valid as taught by Johnson et al. with the priorities between different applications being set and intervals between notifications being controlled by values appropriate for the requesting applications in order to provide an efficient and effective system and method for coordinating notification requests as shown by Hamill-Keays et al. for the purpose of executing a validity check process for determining whether the registration request is valid, in response to the registration request for the care-of-address, wherein the informing unit includes a unit that executes said process for informing, before the validity check process is executed.

Consider claim 6, Hamill-Keays et al. clearly shows and discloses a system that informs the mobile node via the network that a communication request directed to the mobile node has been transmitted from another node, based on stored event information. This reads on the claimed "...apparatus according to claim 1, further comprising a unit that informs the mobile node via the network that the communication

request directed to the mobile node has been transmitted from said another node, based on the stored event information, ..." ("When attempts to contact a mobile terminal directly by different applications are unsuccessful, a control node, such as a Home Location Register (HLR) or a Service Control Point (SCP) within an Intelligent Network (IN), can receive notification requests from these nodes or applications and prioritize them according to the time received and/or the priority of each requesting application." abstract). However, Hamill-Keays et al. fails to teach that the communication request directed to the mobile node is in response to the registration request for the care-of-address. Johnson et al. discloses a list, maintained by each mobile node, recording information for each binding update sent by this mobile node, for which the lifetime of the binding sent in that binding update has not yet expired. This reads on the claimed "...in response to the registration request for the care-of-address" ("When a mobile node receives a packet tunneled to it from its home agent, the mobile node assumes that the original sending correspondent node has no binding cache entry for the mobile node, since the correspondent node would otherwise have sent the packet directly to the mobile node using a Routing header. The mobile node thus returns a Binding Update to the correspondent node, allowing it to cache the mobile node's binding for routing future packets." (see 'Mobility Support in Ipv6', 3.1, Protocol Summary)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the system in which when a mobile node receives a packet tunneled to it from its home agent, the mobile node assumes that the original sending correspondent node has no binding cache entry for the mobile node,

since the correspondent node would otherwise have sent the packet directly to the mobile node using a Routing header and the mobile node thus returning a binding update to the correspondent node, allowing it to cache the mobile node's binding for routing future packets as taught by Johnson et al. with events when attempts to contact a mobile terminal directly by different applications are unsuccessful, a control node, such as a Home Location Register (HLR) or a Service Control Point (SCP) within an Intelligent Network (IN), can receive notification requests from these nodes or applications and prioritize them according to the time received and/or the priority of each requesting application as shown by Hamill-Keays et al. for the purpose of informing the mobile node via the network that the communication request directed to the mobile node has been transmitted from said another node, based on the stored event information, in response to the registration request for the care-of-address.

Consider claim 7, Hamill-Keays et al., as modified by Johnson et al., clearly shows and discloses an apparatus according to claim 1, further comprising a unit that informs, when the communication request, which is transmitted from said another node and directed to the home address, is received in a state in which the mobile node is not connected to the network, said another node via the network that the mobile node is not connected to the network and that when the mobile node becomes communicable, this fact is to be noticed ("In some instances, the MS 20 may not respond to attempts to contact it for a variety of reasons, including being powered off, being in radio shadow, congestion, etc. If the MS 20 cannot be reached, the party or application trying to

contact the MS 20 normally has to retry contacting the MS 20 after a period of time. An alternative to this is for the party or application to request the network 10 to notify it of when the MS 20 is known to be available, for example, at power on, location registration, or contact by another party. This request is normally made to a control point (not shown) in the network 10 which stores data indicating the address of the party or application who requires notification." column 2, lines 5 - 16).

Consider claim 8, Hamill-Keays et al. clearly shows and discloses a method for forwarding a communication request, which is directed to a node and is transmitted from another node, to a network segment to which the node is currently connected. This reads on the claimed "A method of forwarding ... to which the mobile node is currently connected, a communication request, which is transmitted from another node via a network and directed ... to the network segment at the destination of movement ..." ("When attempts to contact a mobile terminal directly by different applications are unsuccessful, a control node, such as a Home Location Register (HLR) or a Service Control Point (SCP) within an Intelligent Network (IN), can receive notification requests from these nodes or applications and prioritize them according to the time received and/or the priority of each requesting application." abstract). A method of storing a communication request when a node is not currently available. This reads on the claimed "storing, when the communication request is received in a state in which the mobile node is not connected to the network, event information indicative of occurrence of the communication request from said another node to the mobile node" ("This request

is normally made to a control point (not shown) in the network 10 which stores data indicating the address of the party or application who requires notification." column 2, lines 13 – 16). A method of informing, based on the stored event information, that the node has become communicable, which is transmitted via the network from the node connected to the network segment. This reads on the claimed "executing, based on the stored event information, a process for informing said another node via the network that the mobile node has become communicable, which is transmitted via the network from the mobile node connected to the network segment at the destination of movement" ("An alternative to this is for the party or application to request the network 10 to notify it of when the MS 20 is known to be available, for example, at power on, location registration, or contact by another party." column 2, lines 10 – 13). However, Hamill-Keays et al. fails to limit the specifics of IP networks. Johnson et al. discloses a method for forwarding a communication request in which each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. This reads on the claimed "A method of forwarding, based on a relationship between a home address allocated to a mobile node and a care-of-address used in a network segment at a destination of movement" ("IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of address. The protocol enables IPv6 nodes to cache the binding of a mobile node's home address with its care-of address, and to then send packets destined for the mobile node directly to it at this care-of address."

abstract). Further, a method of informing, based on the stored event information, that the node has become communicable, in response to a registration request for registration of the care-of-address, which is transmitted via the network from the mobile node connected to the network segment. This reads on the claimed "...based on the stored event information, a process for informing said another node via the network that the mobile node has become communicable, in response to a registration request for registration of the care-of-address, which is transmitted via the network from the mobile node connected to the network segment at the destination of movement" ("After detecting that its link-layer point of attachment has moved from one IPv6 subnet to another (i.e., its current default router has become unreachable and it has discovered a new default router), a mobile node SHOULD form a new primary care-of address using one of the on-link network prefixes advertised by the new router." (see 8.3. Forming New Care-of Addresses)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate IPv6 protocol enabling nodes to cache the binding of a mobile node's home address with its care-of address, and then sending packets destined for the mobile node directly to it at this care-of address as taught by Johnson et al with service control point as shown by Hamill-Keays et al. for the purpose of a method that forwards communication requests directed to a home address of a mobile node and transmitted from another node via a network, to a network segment to which the mobile node is currently connected, based on a relationship between the home address and a care-of-address used in the network segment.

Consider claim 9, Hamill-Keays et al. clearly shows and discloses a method according to claim 8, further comprising a unit that stores the address of the party or application who requires notification. This reads on the claimed "... apparatus according to claim 8, further comprising storing the ...address of the mobile node ..." ("This request is normally made to a control point (not shown) in the network 10 which stores data indicating the address of the party or application who requires notification." column 2, lines 13 - 16). However, Hamill-Keays et al. fails to teach registered care-of addresses. Johnson et al. discloses a system in which each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. This reads on the claimed "... care-of-address of the mobile node on the basis of the registration request" ("Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location." abstract).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method in which each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet and while situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current

location as taught by Johnson et al. with events when a request is normally made to a control point in the network which stores data indicating the address of the party or application who requires notification as shown by Hamill-Keays et al. in for the purpose of storing the care-of-address of the mobile node on the basis of the registration request.

Consider claim 10, Hamill-Keays et al., as modified by Johnson et al., clearly shows and discloses a method according to claim 8 wherein the event information includes an address of said another node that has transmitted the communication request ("When the MS 440 powers on (step 520) and the HLR 430 detects activity, the HLR 430 scans the list of notification requests 435 for the subscriber trying to detect a priority one notification (step 525)." column 4 lines 63 and column 5 line 10).

Consider claim 11, Hamill-Keays et al. clearly shows and discloses a method in which priorities between different applications can be set and intervals between notifications can be controlled to values appropriate for the requesting applications in order to provide an efficient and effective system and method for coordinating notification requests. This reads on the claimed "method for executing a ... process ..., after the validity check process ..." ("Thus, priorities between different applications can be set and intervals between notifications can be controlled to values appropriate for the requesting applications in order to provide an efficient and effective system and method for coordinating notification requests." abstract). However, Hamill-Keays et al. fails to

teach validity checks for determining whether the registration request is valid, in response to the registration request for the care-of-address. Johnson et al. discloses a system for validating registration requests if the packet contains an IP authentication header and the authentication is valid. The authentication header MUST provide sender authentication, integrity protection, and replay protection. The option length field in the binding update option is greater than or equal to the specified length. The sequence number field in the binding update option is greater than the sequence number received in the previous binding update for this home address, if any. The sequence number comparison is performed modulo 2**16. The packet MUST contain a valid home address option. The home address for the binding is specified by the home address field of the home address option. This reads on the claimed "...method for executing a validity check process for determining whether the registration request is valid, in response to the registration request for the care-of-address, ... ("Upon receiving a Binding Update option in some packet, the receiving node MUST validate the Binding Update according to the following tests: The packet contains an IP Authentication header and the authentication is valid [1]. The Authentication header MUST provide sender authentication, integrity protection, and replay protection. The Option Length field in the Binding Update option is greater than or equal to the length specified in Section 4.1. The Sequence Number field in the Binding Update option is greater than the Sequence Number received in the previous Binding Update for this home address, if any. The Sequence Number comparison is performed modulo 2**16. The packet MUST contain a valid Home Address option. The home address for the binding is specified by

the Home Address field of the Home Address option." (see 'Mobility Support in Ipv6', 6.2. Receiving Binding Updates)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a method for validating registration requests if the packet contains an IP authentication header and the authentication is valid as taught by Johnson et al. with priorities between different applications being set and intervals between notifications being controlled by values appropriate for the requesting applications in order to provide an efficient and effective system and method for coordinating notification requests as shown by Hamill-Keays et al. for the purpose of executing a validity check method for determining whether the registration request is valid, in response to the registration request for the care-of-address, after the validity check process determines that the registration request is valid.

Consider claim 12, Hamill-Keays et al. clearly shows and discloses a method in which priorities between different applications can be set and intervals between notifications can be controlled to values appropriate for the requesting applications in order to provide an efficient and effective system and method for coordinating notification requests. This reads on the claimed "method for executing a ... process ..., before the validity check process is executed ..." ("Thus, priorities between different applications can be set and intervals between notifications can be controlled to values appropriate for the requesting applications in order to provide an efficient and effective system and method for coordinating notification requests." abstract). However, Hamill-

Keays et al. fails to teach validity checks for determining whether the registration request is valid, in response to the registration request for the care-of-address. Johnson et al. discloses a system for validating registration requests if the packet contains an IP authentication header and the authentication is valid. The authentication header MUST provide sender authentication, integrity protection, and replay protection. The option length field in the binding update option is greater than or equal to the specified length. The sequence number field in the binding update option is greater than the sequence number received in the previous binding update for this home address, if any. The sequence number comparison is performed modulo 2**16. The packet MUST contain a valid home address option. The home address for the binding is specified by the home address field of the home address option. This reads on the claimed "...method for executing a validity check process for determining whether the registration request is valid, in response to the registration request for the care-of-address, ... ("Upon receiving a Binding Update option in some packet, the receiving node MUST validate the Binding Update according to the following tests: The packet contains an IP Authentication header and the authentication is valid [1]. The Authentication header MUST provide sender authentication, integrity protection, and replay protection. The Option Length field in the Binding Update option is greater than or equal to the length specified in Section 4.1. The Sequence Number field in the Binding Update option is greater than the Sequence Number received in the previous Binding Update for this home address, if any. The Sequence Number comparison is performed modulo 2**16. The packet MUST contain a valid Home Address option. The home address for the binding is specified by

the Home Address field of the Home Address option." (see 'Mobility Support in Ipv6', 6.2. Receiving Binding Updates)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a method for validating registration requests if the packet contains an IP authentication header and the authentication is valid as taught by Johnson et al. with priorities between different applications being set and intervals between notifications being controlled by values appropriate for the requesting applications in order to provide an efficient and effective system and method for coordinating notification requests as shown by Hamill-Keays et al. for the purpose of executing a validity check method for determining whether the registration request is valid, in response to the registration request for the care-of-address, before the validity check process determines that the registration request is valid.

Consider claim 13, Hamill-Keays et al. clearly shows and discloses a method that informs the mobile node via the network that a communication request directed to the mobile node has been transmitted from another node, based on stored event information. This reads on the claimed "...method according to claim 8, further comprising informing the mobile node via the network that the communication request directed to the mobile node has been transmitted from said another node, based on the stored event information, ..." ("When attempts to contact a mobile terminal directly by different applications are unsuccessful, a control node, such as a Home Location Register (HLR) or a Service Control Point (SCP) within an Intelligent Network (IN), can

receive notification requests from these nodes or applications and prioritize them according to the time received and/or the priority of each requesting application." abstract). However, Hamill-Keays et al. fails to teach that the communication request directed to the mobile node is in response to the registration request for the care-of-address. Johnson et al. discloses a list, maintained by each mobile node, recording information for each binding update sent by this mobile node, for which the lifetime of the binding sent in that binding update has not yet expired. This reads on the claimed "...in response to the registration request for the care-of-address" ("When a mobile node receives a packet tunneled to it from its home agent, the mobile node assumes that the original sending correspondent node has no binding cache entry for the mobile node, since the correspondent node would otherwise have sent the packet directly to the mobile node using a Routing header. The mobile node thus returns a Binding Update to the correspondent node, allowing it to cache the mobile node's binding for routing future packets." (see 'Mobility Support in Ipv6', 3.1, Protocol Summary)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the method in which when a mobile node receives a packet tunneled to it from its home agent, the mobile node assumes that the original sending correspondent node has no binding cache entry for the mobile node, since the correspondent node would otherwise have sent the packet directly to the mobile node using a routing header and the mobile node thus returns a binding update to the correspondent node, allowing it to cache the mobile node's binding for routing future packets as taught by Johnson et al with events when attempts to contact

a mobile terminal directly by different applications are unsuccessful, a control node, such as a Home Location Register (HLR) or a Service Control Point (SCP) within an Intelligent Network (IN), can receive notification requests from these nodes or applications and prioritize them according to the time received and/or the priority of each requesting application as shown by Hamill-Keays et al. in. for the purpose informing the mobile node via the network that the communication request directed to the mobile node has been transmitted from said another node, based on the stored event information, in response to the registration request for the care-of-address.

Consider claim 14, Hamill-Keays et al., as modified by Johnson et al., clearly shows and discloses a method according to claim 8, further comprising informing, when the communication request, which is transmitted from said another node and directed to the home address, is received in a state in which the mobile node is not connected to the network, said another node via the network that the mobile node is not connected to the network and that when the mobile node becomes communicable, this fact is to be noticed. ("In some instances, the MS 20 may not respond to attempts to contact it for a variety of reasons, including being powered off, being in radio shadow, congestion, etc. If the MS 20 cannot be reached, the party or application trying to contact the MS 20 normally has to retry contacting the MS 20 after a period of time. An alternative to this is for the party or application to request the network 10 to notify it of when the MS 20 is known to be available, for example, at power on, location registration, or contact by another party. This request is normally made to a control point (not shown) in the

network 10 which stores data indicating the address of the party or application who requires notification." column 2, lines 5 - 16).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mark D. Fearer whose telephone number is 571-270-1770. The examiner can normally be reached on Monday - Friday, 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rafael Perez-Gutierrez can be reached on 571-272-7915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

mdf

RAFAEL PEREZ-GUTIERREZ
SUPERVISORY PATENT EXAMINER
1/4/07